A-F
IFW

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	**Boris BALACHEFF et al.**	Examiner:	Abdulhakim NOBAHAR
Serial No.:	**09/936,131**	Art Unit:	2132
Filed:	September 4, 2001	Our Ref:	B-4295PCT 619055-2
For:	"SMARTCARD USER INTERFACE FOR TRUSTED COMPUTING PLATFORM"	Date:	November 21, 2005
		Re:	***Appeal to the Board of Appeals***

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final rejection, dated August 1, 2005, for the above identified patent application, together with a petition for a one month extension of time pursuant to 37 C.F.R. 1.136(a). Please deduct the amount of $120.00 for the fee set forth in 37 C.F.R.1.17(a)(1) for the extension of time from deposit account no. 08-2025. Please also deduct the amount of $500.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief from deposit account no. 08-2025. Appellants submit that this Appeal Brief is being timely filed, since the Notice of Appeal is being filed concurrently.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present application.

STATUS OF CLAIMS

Claims 1 - 38 and 41 - 61 are the subject of this Appeal and are reproduced in the accompanying appendix. Claims 39 and 40 have been canceled.

STATUS OF AMENDMENTS

An Amendment After Final Rejection has been submitted concurrently. The listing of claims appended hereto presents the claims as amended in this Amendment After Final Rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates generally to systems and methods for allowing a user of a computer to establish that the computer is trustworthy and that its operation has not been somehow corrupted (p. 3 ll. 22-29). The user is in possession of a token such as a smartcard which the user employs to verify that a computer is trustworthy (p. 3 ll. 30-35, p. 11 ll. 3-15). The computer or computing platform is equipped with a trusted component that is tamper-proof (p. 11 ll. 20-24) and that monitors the computing platform to ensure that its trustworthiness has not been subverted, such as by a virus (p. 12 ll. 1-15). The user's token requests the monitoring (trusted) component to provide certain data regarding the operating status of the computing platform and then compares that data with data resident on the token to determine whether the computing platform may be trusted by the user (p. 12 l. 32 – p. 13 l. 5) to engage in some sort of exchange such as a banking transaction (p. 13 ll. 6-11). If the token determines that the computing platform cannot be trusted, it can simply end communication/data exchange with the computing platform (p. 21 ll. 26-28) and/or deny required authorization for application programs running on the computing platform (p. 27, ll. 19-22). If the computing platform can be trusted, the token may cause the computing platform to display a verification message to the user to let the user know that the computing platform may be trusted (p. 28 ll. 15-20).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether Claims 1, 2, 10-32, 38 and 41-61 are patentable under 35 U.S.C. 103(a) over U.S. Pat. No. 5,923,759 to Lee (hereinafter "Lee") in view of U.S. Pat. No. 5,822,431 to Sprunk (hereinafter "Sprunk").

Issue 2: Whether Claims 3-5, 9, 33, 34, 36 and 37 are patentable under 35 U.S.C. 103(a) over Lee in view of Sprunk and further in view of U.S. Patent No. 6,230,266 to Perlman (hereinafter "Perlman").

GROUPING OF CLAIMS

For each ground of rejection which Appellants contest herein and which applies to more than one claim, such additional claims, to the extent separately identified and argued below, do not stand or fall together.

ARGUMENT

Issue 1: Whether Claims 1, 2, 10-32, 38 and 41-61 are patentable under 35 U.S.C. 103(a) over U.S. Pat. No. 5,923,759 to Lee (hereinafter "Lee") in view of U.S. Pat. No. 5,822,431 to Sprunk (hereinafter "Sprunk").

In the on-final Office Action of March 2, 2005, the Examiner rejected Claims 1, 2, 10-32, 38 and 41-61 as unpatentable over Lee in view of Sprunk. In particular, with regards to claims 1 and 48, the Examiner expressed the opinion that Lee discloses all claimed limitations except for a monitoring component that is configured to perform a plurality of data checks on the computing platform, and that Sprunk discloses precisely this limitation. The Examiner further opined that the skilled person would have found obvious to modify Lee as taught by Sprunk because doing so "ensures that the network meets a minimum reliability standard." Appellants respectfully disagree with the conclusions that the Examiner has made with regard to the teachings of the cited prior art and submit that Lee and Sprunk do not in fact teach, disclose or suggest all of the claim limitations of the rejected claims. Therefore, Appellants submit that the Examiner has not established a *prima facie* case of obviousness based on Lee and Sprunk, and the rejection of Claims 1, 2, 10-32, 38 and 41-61 should be overturned on appeal.

In their response to the non-final Action, Appellants discussed at great lengths the differences between the presently claimed invention and the disclosures of Lee and Sprunk, and explained in detail why the Examiner's interpretation of these references was incorrect and further why there is no motivation for the skilled person to attempt to combine these references in the manner alleged by the Examiner. In particular, Appellants noted that Lee does not in fact disclose the claimed token device that operates to make an integrity challenge to the monitoring component and that will not undertake specific actions of which it is capable unless it receives a satisfactory response to the integrity challenge. Appellants explained that there is no teaching in the passage cited by the Examiner nor, for that matter, anywhere else in the disclosure or claims or drawings of Lee that either specifies or even hints at what happens after the smartcard determines that the system is not authentic. Contrary to the Examiner's assertion, Lee does not teach, mention or hint anywhere that the card will not undertake specific actions unless it receives a satisfactory response to an integrity challenge. Lee in fact is concerned with the security of the host computer 100 against malicious code on the smartcard, and teaches only that the host computer and its resident application module may refuse to perform certain actions such as transfer data, etc. (Please see, in particular, discussion at col. 8, ll. 49-67). There is absolutely nothing in Lee that can possibly be understood as teaching that the smartcard may refuse to perform certain actions, under any type of circumstances.

In the final Action the Examiner retorts that "Lee discloses that when a smart card and a computing system authenticate each other (see, for example, col. 3, lines 60-67 and col. 6, lines 60-67) operations such as financial transactions, data transmission and application program execution (see col. 2, lines 40-48, col. 3, lines 32-40 and col. 8, lines 35-60) could be performed that otherwise in the case of an unsatisfactory response (i.e. unauthenticated card or system) would not happen. However, each of the mentioned operations is a specific action." This reply completely and conveniently ignores the important limitation that it is the claimed smartcard (token) that refuses to perform certain actions, whereas Lee teaches that the host computer is the entity that does not take actions such as "financial transactions, data transmission and application program execution." The very language cited by the Examiner makes this abundantly clear:

> Application program 400 resides in the host 170 and/or the application module 150... If verification is

> successful, application program 400 causes processor 156 to receive debit information from the card... Under control of program 400, processor 156 communicates with a system belonging to the user's bank... Numerous different types of application programs can be provided for application program 400, such as credit transaction programs, prepaid-card programs, medical history programs, and welfare benefit programs.

A useful way of looking at Lee *vis a vis* Appellants' invention is to understand that Lee is essentially concerned with the protection of a host computer from being compromised through an interaction with a smartcard, whereas Appellants' concerns run directly contrary and are directed to the security of the smartcard (and its user) and the prevention of a compromised host computer from illegally accessing information on the smartcard.

In their previous response Appellants also objected to the lack of motivation for the skilled person to combine Lee with Sprunk, and noted that there is no network mentioned anywhere in Lee, and thus the skilled person perusing Lee would have no motivation whatsoever to look at a reference directed to network reliability such as Sprunk. In the final Action the Examiner replies that "[o]n the contrary, there are several indications in Lee that the invention is implemented in a distributed computing system (i.e. a computer network)...Therefore, a person skilled in the art can be motivated to implement the teaching of Sprunk for checking integrity of a network member by another network member (i.e. a component in the network) in the system of Lee." This is simply not correct. There is no mention whatsoever of "distributed computing" in Lee, and the passages cited by the Examiner disclose – at most – the fact that the host computer may be equipped with a modem to communicate "with a system belonging to the user's bank (not shown)... to verify that the user's account contains sufficient funds to cover the charge." [col. 8 ll. 53-57] To allege that this fleeting mention of a modem would motivate a skilled person looking to practice the invention of Lee to consult Sprunk's Virtual Authentication Network for Secure Processors "for checking the integrity of a network member by another network member" stretches all credibility. There are no "network members" in Lee. *Ergo*, there are no network members in Lee that would be interested in checking the integrity of "another

network member." This all makes perfects sense, of course, because there is no network in Lee. The alleged "motivation" offered by the Examiner in defense of his untenable combination of these two references defies reason and relies on a completely indefensible interpretation of Lee that flies in the face of the very language of this reference. To argue that because the computer of Lee can communicate with other computers, it is obvious to consider modifying it in accordance with teachings directed to ensuring the integrity of a group of secure processing elements in a communication system borders on the specious and is an ineffectual attempt at justifying what is clearly the Examiner's use of the claims as a roadmap to combining a highly disjointed reading of the prior art references into a semblance of the claimed invention.

For the above reasons, Appellants submit that the rejection of claims 1 and 48 in view of Lee and Sprunk is improper and indefensible, and therefore respectfully request the Board to overturn the rejection of these claims and pass them to issue.

Claims 2-16 depend from claim 1 and claims 49-58 are dependent from claim 48. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion of claim 1, Appellants submit that claims 2-16 and 49-58 are also allowable, and these claims are thus not further individually addressed herein.

With regards to claim 17, Appellants noted in their previous response that Lee does not in fact teach the host computer displaying verification data verifying correct operation of the computer platform, and pointed out that the passage cited by the Examiner discloses nothing more than the host computer requesting the user of the smartcard to enter a PIN in order to gain access to the computer. In the final Action, the Examiner once again cites to the same passage and offers that "the '...system 100 prompts the user to enter a PIN...,' the '...then system 100 determines that the user is authorized and allows the user to gain entry into system 100', and the '...then system 100 determines that the user is not authorized...' in col. 17, lines 52-61 in Lee *are indications of visual display of information on a monitor screen to a person of ordinary skill in the art.*" Appellants are completely befuddled as to how a skilled person could possibly perceive "indications of visual display of information on a monitor screen" from a teaching of the simple act of requesting a pin. At most, it can be understood that the system 100 present to the user a visual display of a question, such as "Please enter PIN." It is the user who provides

information to the system 100 in the form of his PIN; Lee is thoroughly silent as to what information the system 100 provides to the user during this authentication process. Even if accepted at face value, the Examiner's overarching statement blithely ignores the claim language at issue, namely "displaying verification data verifying correct operation of the computer platform" which is a highly specific action that is most certainly not anticipated by the alleged "visual display of information."

Claim 18 stands rejected "as applied to the like elements of claims 1, 13, 14 and 15 stated above." Appellants have addressed the patentability of claims 1, 13, 14 and 15 above, and thus submit that claim 18 is likewise allowable for these same reasons.

Claims 19-24 depend from claim 18. Therefore, in light of the above discussion of claim 18, Appellants submit that claims 19-24 are also allowable, and these claims are not further individually addressed herein.

With regard to claim 25, the Examiner finds that Lee does not disclose a monitoring component performing a monitoring operation of a computer platform in response to a received interrogation request signal, nor the monitoring component reporting a result message to said interface, the result message describing a result of the monitoring operation, but that Sprunk discloses these limitations. Appellants have shown that the Examiner's combination of these two references is completely devoid of any motivation for the skilled person. Furthermore, in their previous reply Appellants explained that Sprunk is directed to members of a network group interrogating one another, and contains absolutely no teaching of a computing entity specifically comprising a monitoring component as claimed. The passages of Sprunk cited to by the Examiner contain nothing but broad descriptions of providing "an opportunity to assess the integrity or trustworthiness of each member" and determining "if the member can successfully complete a secure test operation." There are no specific details disclosed whatsoever regarding such assessments and tests. The Examiner does not reply to Appellants' arguments in the final Action, but rather merely repeats wholesale the rejection as set forth in the first Action, and Appellants have no choice but to respectfully request that the Board kindly consider their earlier arguments and pass claim 25 to issue.

Claims 26-31 depend from claim 25. Therefore, in light of the above discussion of claim 25, Appellants submit that claims 26-31 are also allowable, and these claims are not further individually addressed herein.

With regards to claim 32, the Examiner once again repeats wholesale his earlier rejection, asserting *inter alia* that Lee discloses that by receipt of a satisfactory result message, the token device offers functionality to the application, at col. 8, ll. 49-57. Appellants explained in their previous response that the application program 400 described in this passage is resident on the application module, and has nothing to do whatsoever with any functionality that may be residing on the smartcard. This entire passage is directed to functions performed by the application module, not the smartcard. Furthermore, as previously explained in great detail, Lee does not address anywhere the concept of the smartcard denying functionality access to the host computer under any type of circumstances, but rather the exact opposite. Because the Examiner has not replied to these arguments, Appellants once gain respectfully request that the Board kindly consider their earlier arguments and pass claim 25 to issue.

Claims 33-37 depend from claim 32. Therefore, in light of the above discussion of claim 32, Appellants submit that claims 33-37 are also allowable, and these claims are not further individually addressed herein.

With regards to claim 38, the Examiner again repeats verbatim is previous rejection based on the allegation that Lee teaches at col. 6, ll. 37-52 programming a token device to respond to a received poll signal from an application program, said poll signal received from the computer platform, and the token device receiving a poll signal from the computer platform, and again invokes Sprunk for allegedly teaching the monitoring component performing a verification operation of the computer platform in response to the received signal from the token device. In their previous reply Appellants had directed the Examiner's attention to the previous discussion of Sprunk with regard to claim 25 and reaffirmed their prior traverse, and furthermore noted that, contrary to the Examiner's assertion, there is nothing in this passage that teaches the receipt of a poll signal from the host computer. Because the Examiner has not replied to these arguments, Appellants respectfully request that the Board kindly consider their earlier arguments and pass claim 38 to issue.

In fact, the Examiner has also not deigned to reply to Appellants' arguments for the patentability of claims 42 and 43, and Appellants thus present these arguments herein for the Board's consideration. Specifically, with regards to claim 42, the Examiner cites to Lee col. 7, ll. 17-34 as teaching the token device responding to the poll signal by providing a request for obtaining verification of a state of the computer entity and the token device receiving a result message, the result message describing the result of the verification. Appellants respectfully disagree. The cited passage teaches that the smartcard can verify that data from the host computer is authentic. There is nothing in this passage regarding the receipt of a poll signal, nor anything that could possibly be understood as requesting verification of a *state* of the host computer, which is not the same nor even similar to the described verification of the authenticity of data received from the host computer.

With regards to claim 43, Appellants reaffirm their previous traverse of the Examiner's combination of Lee and Sprunk as lacking proper motivation, and further disagree that generating the message authentication code (MAC) of Lee is the same as the claimed monitoring component establishing an identity of itself. The MAC is generated from data that the monitoring component has transmitted to the smartcard (col. 7, l. 19-22) and a key, and has nothing to do with the identity of the monitoring component but rather is directed to the authentication of the data transmitted to the smartcard.

With regards to claim 44, Appellants wish to reference the previous discussion regarding claim 1, wherein it is explained in detail that Lee does not in fact disclose the smartcard denying any sort of functionality to the host computer for any reason. Appellants therefore submit that claim 44 is also allowable.

Claim 41 depends from claim 44, and is therefore also submitted to be allowable.

Claims 45-47 depend from claims that have been previously addressed, and are therefore also submitted to be allowable.

With regards to claim 59, Appellants reaffirm their previous traverse of the Examiner's combination of Lee and Sprunk as lacking proper motivation, and thus respectfully submit that claim 59 is not in fact anticipated.

Claims 60-61 are dependent from claim 59 and therefore are also submitted to be allowable.

Issue 2: Whether Claims 3-5, 9, 33, 34, 36 and 37 are patentable under 35 U.S.C. 103(a) over Lee in view of Sprunk and further in view of U.S. Patent No. 6,230,266 to Perlman (hereinafter "Perlman").

Each of claims 3-5, 9, 33, 34, 36 and 37 has been addressed above by the discussion of their respective underlying independent claim, and Appellants thus submit that by virtue of these claims' dependencies, they are also allowable and are thus not further individually addressed herein. Appellants therefore respectfully request that the rejection of these claims also be overturned on appeal and that these claims be passed to issue.

CONCLUSION

For the extensive reasons advanced above, Appellants respectfully contend that each pending claim is patentable. Therefore, reversal of all rejections and objections and re-opening of the prosecution is respectfully solicited.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

November 21, 2005
(Date of Transmission)

Alma Smalling
(Name of Person Transmitting)

(Signature)

11/21/05
(Date)

Respectfully submitted,

Robert Popa
Attorney for Applicants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com

Attachments

Claims

1. (original) A system of computing apparatus comprising:

a computing platform having a first data processor and a first data storage means;

a monitoring component having a second data processor and a second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform; and

a token device being physically distinct and separable from said computing platform and said monitoring component,

wherein in one mode of operation, said token device operates to make an integrity challenge to said monitoring component and said token device will not undertake specific actions of which it is capable unless it receives a satisfactory response to said integrity challenge.

2. (original) The system as claimed in claim 1, wherein said token device receives a detailed response to said integrity challenge, and processes said integrity response to interpret said integrity response.

3. (original) The system as claimed in claim 1, further comprising a third party server, wherein a response to said integrity challenge is sent to said third party server.

4. (original) The system as claimed in claim 3, wherein said monitoring component sends a detailed integrity response to a third party server if requested to do so in said integrity challenge.

5. (previously presented) The system as claimed in claim 3, wherein said monitoring component reports a detailed integrity response to said token device and said token device sends said integrity response to said third party server if it requires the third party server to help interpret said detailed integrity response.

6. (previously presented) The system as claimed in claim 3, in which a third party server simplifies said integrity response to a form in which said token device can interpret said integrity response.

7. (previously presented) The system as claimed in claim 6, wherein a third party server sends a simplified integrity response to said token device.

8. (previously presented) The system as claimed in claim 7, operating to add a digital signature data to said simplified integrity response, said digital signature authenticating said third party server to said token device.

9. (previously presented) The system as claimed in claim 1, wherein said monitoring component sends a detailed integrity response to a third party server.

10. (previously presented) The system as claimed in claim 1, in which said token device is requested to take an action.

11. (previously presented) The system as claimed in claim 1 in which said token device requests to take an action.

12. (previously presented) The system as claimed in claim 1 in which said token device sends image data to said computer platform if a said satisfactory response to said integrity challenge is received, and said computer platform displays said image data.

13. (original) The system as claimed in claim 1, wherein said monitoring component is capable of establishing an identity of itself.

14. (original) The system as claimed in claim 1, further comprising an interface means for interfacing between said monitoring component and said token device.

15. (previously presented) The system as claimed in claim 1, wherein said system of computing apparatus is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer platform.

16. (original) The system as claimed in claim 1, wherein a said specific action comprises authorising said computing platform to undertake a transaction on behalf of a user of said system.

17. (original) A system of computing apparatus comprising:

a computing platform having a first data processor and a first data storage means;

a monitoring component having a second data processor and a second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform; and

a token device beingphysically distinct and separable from said computing platform and said monitoring component,

wherein said token device sends an integrity challenge to said monitoring component;

said monitoring component generates a response to said integrity challenge;

if said token device receives a satisfactory response to said integrity challenge, then said token device sends verification data to said computer platform, said verification data verifying correct operation of said computer platform; and

said computer platform displays said verification data on a visual display screen.

18. (original) A computing entity comprising:

a computing platform having a first data processor and first data storage means;

a monitoring component having a second data processor and second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform, said monitoring component being capable of establishing an identity of itself.

interface means for communicating with a token device, said interface means communicating with said monitoring component,

wherein said computing entity is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer platform.

19. (original) The computing entity as claimed in claim 18, wherein on communication between said token device and said interface means, said monitoring component is activated to

perform a monitoring operation on said computer platform, in which said monitoring component obtains data describing an operating status of said computer platform.

20. (original) The computing entity as claimed in claim 18, wherein said interface means is resident substantially wholly within said monitoring component.

21. (currently amended) The computing entity as claimed in claim 18, wherein said interface means ~~comprises~~ is comprised by said computer platform.

22. (original) The computing entity as claimed in claim 18, wherein said interface means comprises a PCSC stack in accordance with PCSC Workgroup PC/SC Specification 1.0.

23. (original) The computing entity as claimed in claim 18, wherein said monitoring component comprises a verification means configured to obtain a certification data independently certifying said status data, and to provide said certification data to said interface means.

24. (original) The computing entity as claimed in claim 18, wherein said interface means is configured to send and receive data according to a pro-active protocol.

25. (original) A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform comprising a first data processor and a first memory means, and a monitoring component comprising a second data processor and a second memory means, said method comprising the

steps of:

receiving an interrogation request signal via an interface of said computing entity;

said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal; and

said monitoring component reporting a result message to said interface, said result message describing a result of said monitoring operation.

26. (original) A method as claimed in claim 25, in which said monitoring operation comprises the steps of:

said monitoring component carrying out one or a plurality of data checks on components of said computing platform; and

said monitoring component being able to report a set of certified reference data together with said data checks.

27. (previously presented) The method as claimed in claim 26, wherein said certified reference data includes a set of metrics to be expected when measuring particular components of said computing platform, and includes digital signature data identifying an entity that certifies said reference data.

28. (original) The method as claimed in claim 25, wherein said step of reporting verification of said monitoring operation comprises sending a confirmation signal to a token device said confirmation signal describing a result of said monitoring operation.

29. (original) The method as claimed in claim 25, wherein said result message is transmitted by said interface to a token

device external of said computing entity.

30. (original) The method as claimed in claim 25, comprising the step of reporting a result of said monitoring operation by generating a visual display of confirmation data.

31. (original) The method as claimed in claim 25, further comprising the step of adding a digital signature data to said result message, said digital signature data identifying said monitoring component; and

transmitting said result message and said digital signature data from said interface.

32. (original) A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform and a monitoring component, said method comprising the steps of:

an application requesting access to a functionality from a token device;

in response to said request for access to functionality said token device generating a request signal requesting a verification data from said monitoring component;

in response to said request for verification, said monitoring component reporting a result message to said token device, said result message describing a result of a monitoring operation;

by receipt of a satisfactory said result message, said token device offers said functionality to said application.

33. (original) The method as claimed in claim 32, wherein said monitoring component sends a detailed integrity response to a

third party server if requested in an integrity challenge by said token device.

34. (original) The method as claimed in claim 32, wherein said monitoring component reports a detailed integrity response to said token device, and said token device sends said integrity response to a third party server if it requires the third party server to help interpret said detailed integrity response.

35. (previously presented) The method as claimed in claim 34, wherein a third party server simplifies said integrity response to a form in which said token device can interpret said integrity response.

36. (original) The method as claimed in claim 32, wherein a third party server sends a simplified integrity response to said token device.

37. (original) The method as claimed in claim 32, further comprising the steps of:

adding a digital signature data to a simplified integrity response, said digital signature data authenticating a third party server to said token device.

38. (original) A method of checking an integrity of operation of a computing entity, said computing entity comprising a computer platform having a first processor means and first data storage means, and a monitoring component comprising a second processor and second memory means, by means of a token device, said token device comprising a third data processor and a third memory means, said method comprising the steps of:

programming said token device to respond to a received poll signal from an application program, said poll signal received from said computer platform;

said token device receiving a poll signal from said computer platform;

in response to said received poll signal, said token device generating a signal for requesting a verification operation by said monitoring component; and

said monitoring component performing a verification operation of said computer platform in response to said received signal from said token device.

39. - 40. (canceled)

41. (previously presented) The token device as claimed in claim 44, said device being configured to be responsive to a poll signal operating in accordance with PC/SC specification 1.0, said token device being capable of initiating a command to be handled by a software stack on the computer entity, in response to said poll signal according to said poll signal according to a proactive protocol.

42. (original) A method of verifying a status of a computing entity, by means of a token device provided external of said computing entity, said method comprising the steps of:

said token device receiving a poll signal;

said token device responding to said poll signal by providing a request for obtaining verification of a state of said computer entity; and

said token device receiving a result message, said result message describing the result of said verification.

43. (original) A method by which a token device can obtain verification of a state of a computing platform by using a monitoring component,

said monitoring component being capable of performing at least one data check on said computer platform, and establishing an identity of itself, and establishing a report of said at least one data check; and

wherein said token device has data processing capability and behaves in an expected manner;

said token device being physically separable from said computing platform and said monitoring component, said token device having cryptographic data processing capability

wherein, said monitoring component proves its identity to said token device and establishes a report to said token device of at least one data check performed on said computing platform.

44. (original) A token device comprising a data processor and a memory device, said token device configured to perform at least one data processing or signaling function:

wherein said token device operates to:

receive an integrity check data from an external source;

if said integrity check data supplied to said token device is satisfactory, then said token device allows a said function; and

if said integrity check data received by said token device is unsatisfactory, then said token device denies said function.

45. (previously presented) A system as claimed in claim 1, wherein said token device is a smart card.

46. (previously presented) A system as claimed in claim 18, wherein said token device is a smart card.

47. (previously presented) A token device as claimed in claim 44 in the form of a smart card.

48. (previously presented) A computing system comprising:

a computing apparatus having a first data processor and a first memory;

a monitoring component having a second data processor and a second memory, wherein said monitoring component is configured to perform a plurality of data checks on said computing apparatus; and

a portable user token being physically distinct and separable from said computing apparatus and said monitoring component,

wherein in one mode of operation, said portable user token operates to make an integrity challenge to said monitoring component and said user computing device will not undertake specific actions of which it is capable unless a satisfactory response to said integrity challenge is provided.

49. (previously presented) The system as claimed in claim 48, wherein said portable user token receives a detailed response to said integrity challenge, and processes said integrity response to interpret said integrity response.

50. (previously presented) The system as claimed in claim 48, in which said portable user token is requested to take an action.

51. (previously presented) The system as claimed in claim 48 in which said portable user token requests to take an action.

52. (previously presented) The system as claimed in claim 48, wherein said monitoring component is capable of establishing an identity of itself.

53. (previously presented) The system as claimed in claim 48, further comprising token interface for interfacing between said monitoring component and said portable user token.

54. (previously presented) The system as claimed in claim 48, wherein said computing system is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer apparatus.

55. (previously presented) The system as claimed in claim 48, wherein the monitoring component is mounted on a common assembly with the first processor.

56. (previously presented) The system as claimed in claim 48, wherein one or more of said data checks comprise a check of the integrity of the basic input/output software for one or more components of the computing apparatus.

57. (previously presented) The system as claimed in claim 48, wherein the portable user token is a smart card.

58. (previously presented) The system as claimed in claim 53, wherein the portable user token is a smart card, and the token

interface comprises a smart card reader.

59. (previously presented) A computing entity comprising:

a computing platform having a first data processor and a first memory;

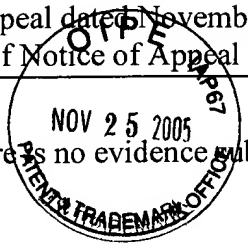
a monitoring component having a second data processor and a second memory, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform,

a communications interface for communicating with a portable user token, said communications interface having a communication path to the monitoring component,

wherein said computing entity is configured such that said monitoring component is adapted to report said data checks to a portable user token connected to the communications interface, said data checks containing data describing a status of said computing platform.

60. (previously presented) The computing entity as claimed in claim 59, wherein on communication between said portable user token and the communications interface, said monitoring component is activated to perform a monitoring operation on said computer platform, in which said monitoring component obtains data describing an operating status of said computer platform.

61. (previously presented) The computing entity as claimed in claim 59, wherein the communications interface is a smart card reader.



There is no evidence submitted with the present Brief on Appeal.

There are no other appeals or interferences related to the present application.